Ask the Cyber Insurgent

By Jan C. Norris, Major, USA

Editorial Abstract: This article won the 2007 Armed Forces Communications Electronics Association Excellence in C4I/ IO Writing Award at the US Army Command & General Staff College. Major Norris provides a critical analysis of the current US military information superiority posture, and recommends a construct to enhance cyber targeting and surveillance.

"Attention in the operations center, attention in the operations center, as of 0730 this morning, our steady theater IO campaign has allowed multi-national forces to achieve information superiority, Victory is imminent."

These words have assuredly never been uttered in any US-led military operations center, nor are they likely to be heard anytime soon in Iraq or elsewhere… at least not with a straight face.

US Joint and Army Information Operations doctrine maintains that achieving information superiority (IS) is a critical factor for success in military operations. Yet for the past four years, US forces have been unable to achieve true IS in connection with Operation Iraqi Freedom (OIF). While possessing an overwhelming edge in information technology to dominate IS, US forces have faltered in one critical area: denying the enemy the ability to collect, process and disseminate an uninterrupted flow of information. Through five years of OIF, the cyber-enabled insurgent has evolved and operated relatively uninhibited using the Internet and media. Both serve as a means of controlling and sustaining momentum, and achieving both tactical success from within by recruiting and mobilizing personnel—and strategic success by influencing international perceptions. If IO are to ever gain status as a decisive form of operational warfare, the US must increase the focus and scope of cyber-surveillance and targeting, so that forces engaged in OIF can deny the cyber-insurgent cyberspace Internet and media access and mobility. To edge closer to achieving a level of IS that directly impacts operational success, we need to establish a Joint Cyberspace Surveillance Targeting Cell (JCST).

Given current tenets of IO doctrine and the ability of US forces to successfully dominate in a majority of the contributors to IS, there should logically be some degree of IS influence on military operational success. But does achieving IS really matter if there is no effective way of denying or mitigating the enemy's medium for information exchange? Is achieving IS even a real concern for today's commanders at the operational level of war?

In Iraq, several distinguished leaders developed innovative techniques and procedures for success in defeating local insurgents on the ground, and engaging the Iraqi populace using IO. Many recognize General David Petraeus and Colonels H.R. McMaster and Dave Putnam for their exceptional ability to conduct successful tactical ground campaigns against the threat, while also and perhaps more critically, engaging the Iraqi leadership and population through sound IO efforts. Despite successful IO and recent positive "surge strategy" trends, there appears to be little attention, focus or mention of achieving IS in after action reviews and lessons learned. A much longer period of time is still needed to achieve the desired end state of Iraqi autonomy, where the insurgency is neutralized and host nation population confident in a stable, legitimate government.

Security Operations Center. (US Army)

The OIF scenario leads back to similar questions; what difference does having IS and conducting IO matter for US forces in Iraq? On the ground, it certainly helps in building trust and confidence between Iraqi local communities and US military and Iraqi forces while having the ability to collect intelligence via advanced systems and technology helps in detecting patterns of activity to track and target the enemy. But are IS and IO helping to mitigate the cyberspace activity sustaining and feeding the insurgency? From a macro view of the information environment, do US forces truly have IS? In most cases the answer is no. Very little is being done to decisively engage the enemy in cyberspace. An insurgent can possess information superiority and an information advantage because he can stay hidden, yet see US forces and decide when to attack. IO efforts and achieving IS can be fleeting; its forces must recognize this and take action to reduce the enemy's IS and operational efficiency. IS in the new operational environment must include denying information helpful to the enemy. A recent posting to an extremist Web site announced a competition to design a new Web page for an Iraqi militant group. The incentive was the chance to fire missiles by remote control at a US military base.

Since 9/11, the growth of extremist-related Web sites has grown significantly to well over 4,500. Many of these sites strongly advocate Al Qaeda's ideology and have evolved into virtual bases for recruiting, training, coordinating attacks, sharing information, fund raising (even using PayPal) and influence. The Internet allows for 'cyber-mobilization' of a variety of ethnic populations around

the globe with similar cultural and ideological causes. It allows many extremist groups to come together quickly in chat rooms and plan and coordinate activities. In essence, the Internet is feeding the cyber-insurgent at a steadily growing pace.

Terrorist groups have applied the same innovation and ingenuity on the Internet as they did in planning the intricate 9/11 attacks, especially in avoiding detection, disruption or destruction of Web site information. Common cyberspace stealth methods include use of encryption, domain name changing, use of proxy servers to obscure locations and "dead dropping," where information is saved as draft messages in fake email accounts. These are accessible to anyone having a password, thereby avoiding transmission and detection. Considering the hundreds of thousands of servers and Internet service providers (ISPs) worldwide, plus the billions of bytes being transferred every second, the insurgent/terrorist has a large playing field to roam—with many choices for data and site hosting. Not surprisingly, many significant Al Qaeda and extremist-linked sites in recent years have been sourced to American ISPs, and their presence was largely unknown to the US providers.

In essence, the Internet is the ideal communications tool for insurgents, and it reflects the framework of their operations: decentralized, anonymous, and offering fast communication to a potentially large audience. It has created a virtual or cyber 'umma' [Arabic for the larger Muslim community], which like the actual umma, encompasses both moderate Muslims and Islamic fundamentalists.

Therefore, regulating cyberspace terrorism and insurgent activity is quite challenging for the US. Law enforcement agencies have, for example, become very efficient in tracking and convicting cyberspace violations of child pornographic laws, but face legal hurdles in the cyber-insurgent fight. Challenges include rights to free speech, getting international partners to take decisive action, and crossing of international borders when targeting cyberspace terrorist/insurgent data. Coupled with the fog of countless on-line insurgent activities, these legal restraints and data flow have left the US government far behind their adversaries in terms of Internet skills and achieving IS. A contributing cause is a lack of cultural and language understanding, and not being able to properly get inside the insurgent's cyberspace 'circle of influence.' Some of the most important US Government agencies tasked with tracking and intercepting Al Qaeda members and activities in cyberspace place little importance on the technological and cultural aspects—and associated skills and knowledge—that are critical to the fight. We must establish a method for better combating cyber-insurgents, one where the Department of Defense is teamed up with Interagency organizations.

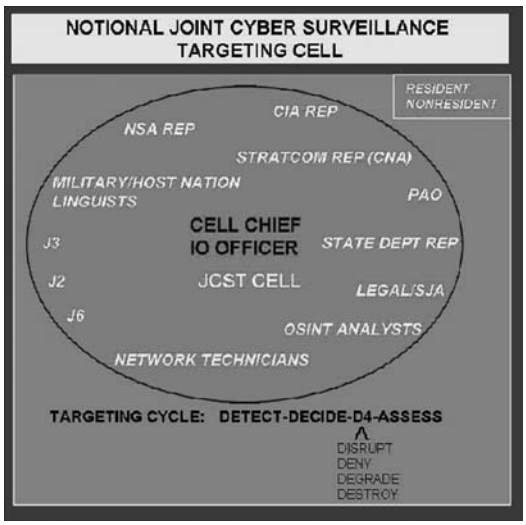

Figure 1. Joint Cyber Surveillance Targeting Cell.

Current IO doctrine addresses Computer Network Attack (CNA) as a subset of computer network operations (CNO), specifically "actions taken through the use of computer networks to disrupt, deny, degrade or destroy (D4) information resident in computers and computer networks." Little else is discussed, as CNA details and processes are sensitive and classified. JP 3-13 does describe a notional joint IO cell, but without specific emphasis on cyberspace surveillance and targeting.

While combating the cyberinsurgent is a complex task akin to "a cat and mouse chase and finding a needle in a haystack," certain deliberate measures can have impact. Creation of a Joint Cyber-Surveillance Targeting (JCST) Cell (Figure 1) inside at the operational level is a start. For example, in the US Central Command (CENTCOM) theater of operations, a JCST cell could be embedded within the MNF-I staff in Baghdad—where it is currently needed most. In other regional combatant commands (RCC) without active on-going combat operations, the cell would function at the RCC headquarters. As this mission clearly falls in the information environment, the fifteen to twenty member cell would be led by an IO officer (O-5 or O-6). Specialties would include interagency cyberspace analyst representation from the CIA, NSA, USSTRATCOM, FBI, and State Department as well as joint military intelligence open-source analysts and linguists, host nation linguists, and information technology specialists (both military and contractor) specializing in wide area network architecture and attack/infiltration. Manning the cell jointly would better educate and train military and government agencies for future joint cyberspace related operations. The JCST cell would continuously scan the Internet for suspected insurgent/terrorist activity, and employ developed technologies, harnessing automation to search and capture Web content. Acting much like a conventional joint targeting cell, the JCST could use a targeting model similar to the Decide-Detect-Deliver-Assess (DDDA) process. However, with Joint Cyberspace Surveillance and Targeting, the process would change to Detect-Decide-D4-Assess, where D4 is "disrupt, deny, degrade or destroy."

JCST cell operations would detect and analyze suspected sites, and if the leadership decides the site is a source contributing to insurgent/terrorist activities—and can be targeted—the cell could take the next step. Network technical specialists would move to take one of four actions: disrupt, deny, degrade or destroy the site, or let it remain as is for further exploitation. Cell efforts could also re-direct individuals

browsing the Web for insurgent sites toward US-constructed sites, providing counterpropaganda to potentially dissuade an insurgent recruit. Decisions to execute any action against a site ultimately rest with the JCST cell chief, unless suspected sites involve external countries where action may involve political sensitivity. In cases where the terrorist site source or host is outside the US, and targeting the associated network or server would impact other important non-insurgent users or organizations (i.e. a banking network), the cell would use a target nomination process. The JCST State Department rep would use Department of State channels to contact the source country for targeting clearance. This approval process would need to carefully avoid compromising US intelligence gathering techniques. Once a site is targeted the cell would make follow on assessments, revisiting ISPs with a history of known or unknown insurgent hosting, to track any recurring patterns. When possible, the JCST would collect and target individual webmasters who are building and creating such sites. Though the scope of targeting such individuals goes beyond the capabilities of the JCST cell proposed here, the information collected would be passed on to appropriate State Department, law enforcement or military officials for action. International support is essential for denying service, particularly in developing countries with known cyberspace terrorist activity and weak governments.

US Government and military personnel may quickly refute the JCST idea as 'double work,' given what the Joint Functional Component Command-Network Warfare (JFCC-NW) and other DOD CNO teams already provide. However, few if any such cells exist with the necessary mix of military and interagency expertise collocated in one spot. Having the cell forward, on the ground in a combat theater of operations may also seem pointless given current communications reach capabilities; yet it is vital. A forward point of presence optimizes speed of decision for establishing linkages, from cyber-insurgent planning, training and recruiting activities, to insurgent activities on the ground. Forward presence also allows direct 'face-to-face' access with the theater commander (MNF-I) and joint/coalition staff. Further, targeting cell personnel can gain a much better situational understanding of insurgent operations by being 'in the culture.' They get a better perspective on insurgent motivation by having host nation personnel available to translate both cultural and linguistic aspects of extremist website content. Additional JCST cells could be positioned in different countries within the theater, where languages and cultures vary and regionally-specific specialist staffing is appropriate. Over time, given proven quantitative measures of effectiveness, theater commanders could track 'cyberspace targeting' as a line of operation contributing to defeat of the enemy center of gravity—and protecting coalition forces and missions.

Many consider the power of the Internet as a means for global information sharing, communication and creation of virtual communities among the most important innovations of the past century. Yet this same interconnected network of worldwide computers, switches and servers, and the cyberspace contained within, has equal potential as a tool for enabling terrorism and death. As enemies of the United States continue to overtly attack its military technological strengths through asymmetric and insurgent warfare, they will also continue to exploit the power of the Internet to extol their ideology and kill Americans. Are information operations a decisive form of operational warfare? If one were to ask the cyber-insurgent, the answer right now is *yes*. Their operational efforts in cyberspace have been decisive for tactical success. In his September 2007 report to Congress on the situation in Iraq, General Dave Petraeus noted "the need to contest the enemy's growing use of that medium (cyberspace) to spread extremism" and that "regional, global and cyberspace initiatives are critical to success." Bridging the gap between the Interagency and military, the proposed JCST cell is an IO organization with potential to neutralize and defeat the cyber-insurgent by bringing together the right mix of personnel to decisively combat insurgent cyberspace activity. Positioned forward in the combat theater, the JCST cell will be immersed in the target culture, to better link operational insurgent activities in cyberspace to tactical actions on the ground. Since OIF began, the relevance of IO, achievement of information superiority, and which side truly has the information advantage all remain in question. By enabling US forces through a deliberate process for targeting and denying enemy information flow in cyberspace, the JCST cell could well prove IO as a decisive form of operational warfare. We may still earn shouts of 'imminent victory' in the theater operations center… with a straight face.